HARROGATE LADIES' COLLEGE & HIGHFIELD

Independent School for Girls Aged 2 to 18 and Boys Aged 2 to 11

HARROGATE LADIES' COLLEGE PUPIL ONLINE SAFETY POLICY AND ACCEPTABLE USE OF ICT

Highfield Pre School, Highfield and College

SLT Responsibility: Joanna Fox

Governor Committee Review: Pupil Welfare

Review Cycle: Annual

Next Review Date: September 2025

1. Introduction

This policy applies to the Harrogate Ladies' College Family of Schools – Highfield Pre-School, Highfield and College - hereafter referred to as "the School".

This Policy is published on the School Intranet and the School website.

The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote online safety.

When this policy is updated, a new version is provided to all pupils electronically, is published on the website and stored in the School's Policy folder. Paper copies are always available on request from the Senior Deputy.

The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is constantly changing. In order to ensure the School provides a safe environment for learning, we adhere to the following principles:

- Online safety is an essential part of safeguarding and the School has a duty to ensure that all pupils and staff are protected from potential harm online
- Online safety education is an important preparation for life. Pupils should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online.

The purpose of the online safety policy is to:

- Safeguard and protect all members of the school's community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example, pornography, racist or radical and extremist views and, in some respects, fake news
- **Contact**: being subjected to harmful online interaction with other users; for example, children can be contacted by bullies or people who groom or seek to abuse them
- **Commercial exploitation**: for example, young people can be unaware of hidden costs and advertising in apps, games and website
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying

Scope

This policy applies to all staff, including teachers, support staff, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as

'staff' in this policy) as well as pupils and parents/carers. It applies to the whole school, including the Early Years Foundation Stage.

This policy applies to the use of all school systems, the internet and the use of technology, and any fixed/mobile electronic technologies and associated software that pupils have access to for personal and school use that might pose online safety risks during a school day. Together with any use at any time, whether on or off School premises, which affects the welfare of other pupils or where the culture or reputation of the School are put at risk. This includes, but is not limited to, online safety behaviour such as cyber-bullying, which may take place outside the School, but is linked to membership of the School. The School will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that takes place out of school.

Pupils are responsible for good, responsible, behaviour on the School network and the Internet, just as they are in the classroom or in a school corridor. General school standards and procedures apply to all who make use of the School's facilities and equipment.

Alongside this policy, in times of full or partial School closure the Remote Education Policy must be adhered to as well. The Remote Education Policy can be accessed on the School website and via the School Intranet. All pupils are given an electronic copy of this policy when they join the School and when significant updates occur.

Staff are also subject to separate policies which forms part of their contract of employment.

See Appendices for acceptable use protocols.

2. Links to other policies

This policy links with a number of other policies, including:

- *Safeguarding and Child Protection Policy*
- *Data Protection Policy*
- *PSHE Policy*
- *Behaviour Policy*
- *Anti-Bullying Policy*
- *Acceptable Use Agreements* (staff and pupils)
- *Remote Education Policy* (when appropriate)
- *Staff Handbook*
- *Staff Code of Conduct*

3. Roles and Responsibilities

- Joanna Fox is the Designated Safeguarding Lead (DSL) responsible for online safety. Sam Pickard is the named Deputy Designated Safeguarding Lead (DDSL) responsible for Early Years Foundation Stage (EYFS).
- ***All*** members of the community have important roles and responsibilities to play with regard to online safety:

The Proprietor (Governors):

The School's Governing Board (GB) has a responsibility to ensure the school has a whole school approach to safeguarding and that all systems, processes and policies operate with the best interests of the child at their heart. The GB should be kept informed of online safety policy and practice via the termly Pupil Welfare safeguarding report.

The Principal:

- Has overall responsibility for online provision in school
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with the School's and national recommendations and requirements
- Ensures the School follows policies and practices regarding online safety (including the *Acceptable Use Agreement*), information security and data protection
- Determines the School's internal policy on the use of personal devices and mobile phones
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Supports the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities
- Ensures all staff receive regular, up to date and appropriate online safety training
- Is aware of what to do in the event of a serious online safety incident, and will ensure there are robust reporting channels for online safety concerns, including internal and national support
- Ensures that online safety practice is evaluated regularly in order to identify strengths and areas for improvement

The Designated Safeguarding Lead (DSL):

- Takes lead day-to-day responsibility for online safety (including understanding the filtering and monitoring processes and systems in place)
- Monitors changes in legislation, policy and government guidance; helps to coordinate further action and minimise the risk of non-compliance with respect to ISI inspections
- Promotes an awareness of, and commitment to, online safety throughout the school community
- Ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement
- Ensures that appropriate filtering and monitoring is in place and takes all reasonable precautions to ensure that users can only access appropriate material
- Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate
- Keeps the online safety component of the curriculum under review, in order to ensure it remains up to date and relevant to pupils

- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate
- Ensures all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Monitors pupils' internet usage, taking action where appropriate
- Reviews and responds to notifications or alerts generated by the filtering and monitoring system, or other incidents of online behaviour that may indicate a safeguarding concern
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends
- Reports regularly to the Principal and SLT on matters on online safety, current issues, developments in legislation etc and termly to the Safeguarding Governor

Staff managing the technical environment, IT Support

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst ensuring learning opportunities are maximised
- Keep up to date with the School's online safety policy and technical information in order to carry out their online safety role effectively, and to inform and update others as relevant
- Provide technical support to the DSL in the implementation of online safety procedures
- Ensure that the School's filtering policy is applied and updated on a regular basis, and oversees the School's monitoring system
- Report any filtering breaches or other online safety issues to the DSL, Privacy Officer and Principal, as appropriate
- Ensure that any safeguarding concerns are reported to the DSL, in accordance with the School's safeguarding procedures.

All school staff:

- Read, adhere to and help promote the *Online Safety Policy*, acceptable use agreements and other relevant school policies and guidance
- Understand their role and responsibility regarding filtering and monitoring
- Take responsibility for the security of school systems and the data they use, or have access to ensuring that they adhere to the School's GDPR Policy ;
- Create secure passwords with at least 8 characters and at least one number with either a capital or a symbol. Staff must never share their passwords.
- Model safe, responsible and professional behaviours in their own use of technology;
- If staff wish to download bespoke software links, this must be requested, and processed, by the IT Support Team
- Staff are not permitted to use USBs, or other external storage devices. If staff have a storage device that they want to access, this must be requested, and processed, by the IT Support Team;

- Embed online safety in their teaching and other School activities, so it is the golden thread that runs through the curriculum
- Supervise, guide and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities, if relevant)
- Have a up to date awareness of a range of online safety issues and how they may be experienced by children in their care
- Identify online safety concerns and take appropriate action by reporting to the DSL
- Know when, and how, to escalate online safety issues
- Take personal responsibility for professional development in this area

Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities):

- Engage in age-appropriate online safety education opportunities
- Read and adhere to the School *Acceptable Use Agreement* (See Appendix 8)
- Respect the feelings and rights of others both on and offline, in and out of school
- Take responsibility for keeping themselves and others safe online
- Report to a trusted adult, if there is a concern online
- All pupils should create secure passwords, with at least 8 characters and at least one number with either a capital or a symbol. Pupils must never share their passwords with others and must ensure that they log off when leaving their PC.

Parents and carers:

- Encourage their children to adhere to the School's *Acceptable Use Agreement* (See Appendix 8)
- Support the School in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home
- Model safe and appropriate use of technology and social media, including seeking permissions before taking and sharing images of pupils other than their own children
- Identify changes in behaviour that could indicate their child is at risk of harm online
- Seek help and support from the School, or other appropriate agencies, if they or their children encounter risk or concerns online
- Use School systems, such as learning platforms, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

External groups/visitors:

- Any external individual or organisation must sign an *Acceptable Use Agreement* prior to being given individual access to the School network. Access must only be given if deemed necessary.

4. Education and Engagement

Education and Engagement with Pupils

The School curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety across the curriculum, including the PSHE, RSE and Computing programmes of study, covering use both at School and at home
- Reinforcing online safety messages whenever technology or the internet is in use
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum
- Educating pupils in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation
- Teaching pupils to be critically aware of what they see online and show how to validate information before accepting its accuracy
- Teaching pupils to respect and adhere to principles of academic integrity. This includes understanding the importance of producing their own, independent work, being honest and transparent about any use of source material or applications, understanding and respecting copyright, and using appropriate referencing conventions
- Supporting pupils in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

The School will support pupils to read and understand the *Acceptable Use Agreement* (AUA) (See Appendix 8) in a way which suits their age and ability by:

- Discussing the AUA and its implications during form time and in computing lessons. Reinforcing the principles via display, classroom discussion etc.
- Informing pupils that networks and internet use will be filtered for inappropriate content and monitored for safety and security purposes and in accordance with legislation
- Recognising positive use of technology by pupils

Training and engagement with staff

The School will:

- Provide and discuss the *Online Safety Policy* and staff *Acceptable Use Agreement* with all members of staff as part of induction
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- Make staff aware that school systems are monitored and activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices during induction and as regular updates
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school

- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and engagement with parents and carers

Parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings and parent guides
- Informing parents about what the school asks pupils to do online, and who they will be interacting with
- Drawing parents' attention to the school online safety policy and expectations in newsletters and on the website
- Requiring parents to discuss the implications of the AUA with their children.

5. Reducing Online Risks

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

- Regularly review the methods used to identify, assess and minimise online risks
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- Ensure, through online safety education and the school AUAs, that pupils know that the School's expectations regarding safe and appropriate behaviour online apply whether the School's networks are used or not

6. Safer Use of Technology

Classroom Use

The school uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platforms
- Cloud services and storage
- Email and messaging
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras
- Virtual reality headsets
- Artificial intelligence

- Supervision of pupils will be appropriate to their age and ability
- All devices should be used in accordance with the School's AUAs and with appropriate safety and security measures in place.
- Members of staff should always check websites, tools and apps thoroughly for suitability, reliability and trustworthiness before their use in the classroom, or recommending for use at home.
- Staff and pupils should consider copyright law before using internet-derived materials and should, where appropriate, comply with license terms and/or acknowledge the source of information.

7. Artificial Intelligence

Artificial intelligence (AI) is changing the way we use technology. With AI constantly evolving, it is important to keep our safety a number one priority. The government has a white paper in progress about how it will regulate AI, but schools must be prepared to keep their pupils safe during this evolution and change.

There are clear benefits of AI. It can:

- provide tailored responses;
- support to develop ideas and knowledge;
- process information and instructions quickly; and
- save time and support to reduce workload.

There are, however, limitations to AI:

- the responses can be harmful, biased or inaccurate;
- mistakes can still be made;
- it is evolving rapidly and, therefore, new challenges will emerge; and
- there are current gaps within safeguarding and regulation.

In School, our pupils must be aware of the following ways to stay safe online. These will be taught through form time, PSHE and computing lessons:

- Understand the limitations: be aware that AI is an imperfect technology and pupils must still apply critical thought to any response it creates
- Talk through concerns: pupils should be supported through AI so, if something harmful is seen, they have the confidence to talk it through with a trusted adult. Examples of potential concerns are: deep fakes and impersonation; harassment and bullying; criminality, coercion and grooming; and exploitation
- Keep personal information secure: pupils should not feel inclined to input any personal or sensitive information into an AI tool
- Be aware of security risks: AI can lead towards improved approaches towards scamming and cyber attacks, so cyber-security must remain a high priority for the whole school

As AI continues to develop, it is useful to acknowledge the impact and to bring these discussions into the classroom. Pupil safety must remain a priority, so staff should support them as they begin to explore AI.

8. Filtering and Monitoring

- All school systems are protected by an internet filter. All incoming and outgoing data are screened by the filter that provides real time filtering and protects both the networks and users from malicious websites and internet threats. It, along with anti-virus software prevent a wide range of unwelcome material and viruses from being available in the School while at the same time allowing access to material of educational value. The policy determining filtering is managed centrally with different levels being applied depending on age group.
- The system logs all internet access on the School system and these logs can be accessed by the DSL for monitoring purposes. Flagged terms will also trigger alerts which the DSL may investigate. Concerns identified will be managed according to the nature of the issue
- Email messages are scanned for malicious content and profane language between pupils or staff to pupils. Email traffic between pupils is not scanned as a matter of course, but if concerns about contacts between pupils are raised, then a record of messages may be retrieved.
- All members of staff are, however, aware they cannot rely on filtering and monitoring alone to safeguard pupils: effective classroom management and regular education about safe and responsible use is essential
- Users are informed that use of School systems is monitored and that all monitoring is in line with data protection, human rights and privacy legislation.

Dealing with filtering breaches

The School has a clear procedure for reporting filtering breaches:

- If pupils discover unsuitable sites, they will be required to alert a member of staff immediately
- The member of staff will report the concern (including the URL of the site if possible) to the DSL
- The breach will be recorded and escalated as appropriate
- Any material the school believes is illegal will be reported immediately to the appropriate agencies, such as Internet Watch Foundation (IWF), the Police or Child Exploitation and Online Protection (CEOP).

9. Managing Personal Data Online

Personal data will be collected, processed, stored and transferred and made available online in accordance with the *General Data Protection Regulations* and the School's Privacy Notices. Full information can be found in the School's *Data Protection Policy.*

10. Social Media

School curriculums are designed to provide a well-rounded education that goes beyond academic subjects and includes the development of social skills and pastoral support. Online services that support personal, social, health, peer support and extracurricular activities are considered to form part of this.

The use of social media will only be facilitated for pupils under the age of 16 where this is for the purpose of delivering the curriculum. Where the terms of service of a social media platform advise they are unsuitable for a child below a defined age, we will abide by these restrictions.

Expectations

- The term social media includes, but is not limited to: blogs; wikis; social networking sites; forums; bulletin boards; online gaming apps; video/photo sharing sites; chatrooms; and instant messenger
- All members of the School community are expected to engage in social media in a positive, safe and responsible manner at all times.

Staff Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites is discussed with staff as part of staff induction and is revisited and communicated via regular staff training opportunities
- Staff are not permitted to be in contact with pupils on any form of social media. All online communications between pupils, and staff, should be done through school and pupil HLC emails.
- Safe and professional behaviour is outlined for all members of staff as part of the *staff Code of Conduct* and the staff *acceptable Use Agreement.*

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of online safety education, via age-appropriate sites and resources
- The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age and inform parents about the age restrictions at Parent Guides as appropriate
- The school will control pupil access to social media whilst using school-provided devices and systems on site:
    - Pupils up to Lower 5 are not permitted access to mobile devices during the School day and, therefore, do not have access to social media sites
    - The use of social networking sites such as Facebook, Twitter, qq.com or similar sites is prohibited during the school day. Access is only available between 7.00am and 7.30am and after 7.00pm and is restricted to pupils in Upper 5 or older
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary action and/or removal of internet facilities

- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

11. Use of Personal Devices and Mobile Phones

The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: *Anti-Bullying*, *Behaviour,* and *Safeguarding and Child Protection*.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. The school accepts no responsibilities for the loss, theft, damage or breach of security of such items on school premises
- Mobile phones are only permitted to be used by Upper 5 and Sixth Form pupils, in form rooms, the U5 Common Room and the Sixth Form Centre. All other pupils should use reception to contact home, or use their mobile phone with explicit permission from a member of staff.
- The sending of abusive or inappropriate messages/content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt according to the *Behaviour Policy.*
- All members of the community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school *Behaviour* or *Safeguarding and Child Protection* policies.
- Please see also *Appendix 3 Mobile Phone Protocol*

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that the use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as: *Safeguarding and Child Protection* and *Acceptable Use Agreements*.
- Images of pupils (other than a member of staff's own children) must not be stored on personal devices. Any image taken on personal devices must be transferred to School systems as soon as reasonably possible and the personal copy permanently removed. Staff are advised to take care to remove any copy which may have been backed up to a cloud service.
- This also applies to the EYFS setting. Throughout the setting all persons in the EYFS are required to adhere to the *Acceptable Use Agreement* on the use of mobile phones and cameras: that is, that images of pupils must not be stored on personal devices. Any images taken on personal devices will be transferred to school systems as soon as reasonably possible and the personal copy permanently removed.

(NB Please see *Safeguarding and Child Protection Policy* for further information)

Pupils' Use of Personal Devices and Mobile Phones

Pupil will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

NB Please see Appendices 2 and 3 below for BYOD and mobile phone protocols.

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the School's *Acceptable use Agreement* and other associated policies, such as *Anti-Bullying* and *Safeguarding and Child Protection policies*
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of school policy.

12. **Responding to Online Safety Incidents and Concerns**

- All members of the School community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting/sharing of nudes and/or semi-nudes), self-generated images of sexual abuse as a result of online grooming, cyberbullying and illegal content (*Please see Appendix 5 for managing allegations of cyberbullying)*
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- If the school is unsure how to proceed with an incident or concern, the DSL will seek legal advice
- Where there is suspicion that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised.

Concerns about Pupils' Welfare

- The DSL will be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern – *please see Appendix 7 for the Online Safety Incident Reporting Form*
- The DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

13. Misuse

- Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the relevant policies and procedures and according to the nature of the complaint
- Any complaint about staff misuse will be referred to the Principal
- Pupils and parents are informed of the School's complaints procedure.

14. Useful Links and Sources of Advice

- Teaching Online Safety in Schools (DfE)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Harmful online challenges and online hoaxes (DfE)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Self-generated child sexual abuse (IWF)
- Generative artificial intelligence in education (DfE)

13.1 National Organisations

- Action Fraud: www.actionfraud.police.uk
- CEOP: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation: www.iwf.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- Childline: www.childline.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

15. Monitoring and Review

All serious online safety incidents will be logged. The Senior Deputy has responsibility for the implementation and annual review of this policy and will consider the record of online safety incidents and new technologies, with the Safeguarding team where appropriate, to decide whether or not existing security and e-safety practices and procedures are adequate.

The school will monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice

The policy framework will be reviewed by the DSL at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place

Version control

Date of last review of this policy	September 2024
Date for next review of this policy	September 2025
Policy owner (SLT)	Senior Deputy
Policy owner (Proprietor)	Dame Francine Holroyd

Appendix 1 Use of the School Network and Internet

Computer storage areas, personal laptops and other portable storage devices will be treated as areas of personal storage. On entry to the School, pupils are assigned a folder on the School network in which work may be stored. Users have responsibility to ensure that the folder is managed and that they are always able to save new documents.

Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on laptops or servers or disks would always be private, nor that they might hide materials they have downloaded. The School reserves the right to access their user-area and personal devices and any other forms of storage medium e.g. CD, DVD, USB device, in their possession if it has grounds to suspect there may be inappropriate material on them.

The following are not permitted:

- USBs or other external storage devices. In some specific subjects, there may be instances when pupils are required to use an external storage device e.g. an SD card could be required in photography; when this is the case teachers will inform pupils and the IT Support team. If pupils have a storage device that they want to access, this must be requested, and processed, by the IT Support Team;
- Damaging, degrading or disrupting computers, computer systems or computer networks or performance;
- Violating copyright laws;
- To share their passwords or use others' passwords;
- Trespassing in others' folders, work or files;
- Intentionally wasting resources;
- Any act which results in upheld complaints to, or legal action against, the School;
- Using the School network for illegal activity;
- Viewing, retrieving, downloading or sharing any material which in the reasonable opinion of the Principal is unsuitable.
- Plagiarism, for example presenting documents compiled from the internet, AI or School network as being the pupil's own work;
- Changing any of the computers' default settings, such as screensavers, backgrounds, folders, icons;
- Installing any software whatsoever. If pupils have a software that they want to access, this must be requested, and processed, by the IT Support Team;
- Circumvention of security or accounting provisions. **The use of routers or dongles is banned in School, the access to wifi rendering these devices unnecessary and a security risk to the School network;**

- **All VPN use is strictly forbidden when using the HLC network;**
- Malicious damage to or tampering with any system on the School network or changing of data;
- Transmission, creation or possession of threatening, extremist, defamatory or obscene material;
- Gaining unauthorised access to resources or websites by the use of internal/external wireless modems. Use of such devices to gain unfiltered access to the Internet is strictly forbidden.

Email

On joining HLC, all pupils are provided with an '@hlc.org.uk' email account, subject to parent/guardian approval. This is the core mode of electronic communication between staff and pupils. Pupils are encouraged to use this account and to check it on a daily basis. All emails should be formal and of a professional nature.

Pupils should not communicate with staff using private email accounts. Private email addresses should only be used by the school as part of HLC communication and after the release of examination results, once the pupil has officially left HLC. Until a pupil has left HLC, staff may only communicate with a pupil via school email accounts.

All emails from, and to, the pupil's @hlc email account are subject to the same standards applied elsewhere in this policy. Pupils should follow the guidelines of Use of the School's Network and Internet, Section 0 above. Pupils should be aware of issues related to 'cyber-bullying' and sanctions as outlined in this policy, Section 10 and 18 below.

Use of Social Networks

- The use of social networking sites such as Facebook, Twitter, qq.com or similar sites is prohibited during the school day. Access is only available between 7.00am and 7.30am and after 7.00pm and is restricted to pupils in Upper 5 or older;
- Pupils must never make contact or chat to anyone who is not known to them and only invite known friends to chat rooms or alike;
- Pupils should only accept friendship requests from people they know in real life;
- 'Friend' requests must not be made to or by members of the School's staff;
- Pupils must consider how the images they share or comments they make may be used or viewed by others. Abusive or bullying language must never be used, nor should any other inappropriate language or comments be made;
- Pupils must not make comments about the School, staff members, other pupils or any other person that could be considered as defamatory or which could bring the School into disrepute. Behaviour of this kind will result in disciplinary action being taken in accordance with this policy and the School's Behaviour Policy;

- Inappropriate use of social networking sites may be reported to the site hosting it and inappropriate posts removed.

Appendix 2 Bring Your Own Device (BYOD)

A "device" includes, but is not limited to, laptops, tablet computers, iPods and mobile phones.

Pupils in Highfield Pre-School and Highfield are not permitted to bring any mobile electronic device onto the School premises without the express permission of a member of staff. All other pupils must comply with the guidelines below specifically relating to BYOD.

The School is fully committed to enabling all pupils to access technology to enhance Teaching and Learning, within a safe and secure environment at Harrogate Ladies' College. Technology is an important element of HLC's teaching and forms an integral part of a modern curriculum. The School seeks to raise the standard of each pupil's digital competence through regular opportunities to use technology within their studies.

There are three IT suites and numerous resource and study areas equipped with computers which pupils can use.

Lower School Users of BYOD:

Pupils in Upper 3 and Lower 4 are not permitted to bring their own device into School. Boarding pupils are expected to leave their device in their Boarding Houses during the School day. If a pupil in Upper 3 and Lower 4 is found with a device in School, during the day, they will receive an instant detention, which will be held on Friday after school, 4.45 to 5.45.

Exceptions to this are:

1. Pupils who have obtained prior permission to bring in a device from the Learning Support Team. This permission is specific to the individual;
2. When a teacher asks a particular class or set to bring in a specific device for a project. The device must only be used in the specified lessons, with teacher supervision.

Pupils in Upper 4 may bring in their devices for use in lessons and/or prep.

- Devices may only be used with staff supervision and permission to use a device must always be requested. If a pupil in Upper 4 is using their device without permission, this will result in an instant detention on Friday after school, 4.45 to 5.45.
- A pupil's device must be password protected and insured. The School requests all pupils store their devices within their lockable space when they are not in use in lessons.

Middle School and Sixth Form Users of BYOD:

Middle School and Sixth Form may bring their own device into School, for use during the School day (For Lower 5 pupils, this does not include a mobile phone).

These devices need to be password protected and insured. The School requests all pupils store their devices within their lockable space when they are not in use in lessons.

Recommended software for BYOD

- Teaching resources are held largely via the Learning Platform, VLE, which is available both in school and also from home

- HLC's aim is to ensure that resources are available to any of the standard web browsers. HLC's VLE and email systems hlcorguk.sharepoint.com/sites/hlchome are accessible remotely via a web browser.
- The pupil's device must have a modern web browser such as Edge, Google Chrome, Firefox or Safari.
- The device should have software compatible with the latest Microsoft Office suite of programs.
- All devices must have a suitable Internet Security system installed to guard against virus infection and any hacking attempts. The mobile nature of devices mean they are also likely to be used at home and at wireless hotspots where risks for hacking and virus infection is much greater.
- The school network is secure and has several levels of virus protection. HLC uses Sophos to prevent school-owned devices being infected. Sophos is used as the school's Internet filtering and firewall system.
- Pupils will only be able to access the internet via the school wifi and no VPNs, dongles/4G mobile networks are acceptable for use in school.

Recommended device for BYOD

- The cost and size of laptops and tablets can vary dramatically. HLC recommends that devices weigh less than 2kg, and have a screen smaller than 15" but bigger than 9". The School recommends devices which have a suitable keyboard for longer term use. Pupils are expected to have a protective case for their device, and details of the device including serial number, make and model should be kept in case of any problems.
- The device should have battery capable of lasting the school day and should be brought into school fully charged.

General Principles for mobile devices:

- The downloading of programs to these devices is the responsibility of the user and the School cannot monitor or accept any responsibility for any programs that are installed or problems that an installation might cause. The downloading of programs to a personal laptop is the responsibility of the user and the School cannot monitor or accept any responsibility for any programs that are installed.
- Pupils must not use their own devices in lessons unless authorised by a subject teacher and only then for the purpose of school-related work.
- Pupils may only connect their own devices to the School's network. Access to the internet via a mobile service is not permitted on School premises.
- Under no circumstances should School computers, printers or other devices be detached from the network to make way for a pupil's own device.

- Pupils are responsible for the material that exists on, or is accessed via, their own devices. The Network Services Department is empowered to scrutinise and, if necessary, retain for further investigation, any device which is or has been attached to the network. All rules of usage for Internet access and computer usage as set out in this policy continue to apply.
- It is the responsibility of the owner to ensure that a licence is in place for all software installed on the device.
- The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto school premises, including those that have been confiscated or which have been handed in to the School Office or Examinations Officer.
- Pupils must not use mobile electronic devices in any manner which in the reasonable opinion of the Principal is inappropriate. When deemed appropriate devices may be searched, for further information, consult the School's Behaviour Policy.

Failure of pupils to follow the guidelines as laid out above will lead to the immediate confiscation of the device, and further disciplinary action being taken. Depending on the breach, disciplinary action could include: misdemeanours (-5), long term removal of device privileges, detention or suspension from school, (internal or external).

Appendix 3 Mobile phone protocol

Some pupils walk to and from school each day and may therefore wish to carry a mobile phone with them.

- Pupils from Upper 3 to Lower 5 must hand their mobile phone in as they enter the School via the Quad entrance at the start of the school day. These can be collected before the pupil leaves at the end of the school day. If a Lower School or Lower 5 pupil is found to have a phone on their person during the school day they will receive a detention on Friday after school, 4.45 to 5.45.
- Pupils in Upper 5 may keep mobile phones about their person but they must be turned off during lesson times.
- Upper 5 may use the phones at lunch times between 13.30 – 14.00 in the Upper 5 Common Room. If pupils in Upper 5 are on their phones outside of these designated areas, their phone will be confiscated. The pupil will receive 1 misdemeanour and the phone must be handed into the Head of Year for the following 2 weeks.
- Pupils in the Sixth Form may keep their mobile device about their person but should only use them outside lesson time unless with the permission of the staff member for that lesson.
- Sixth Form pupils must only use their phones within the Sixth Form Centre. As soon as Sixth Form pupils descend from the Sixth Form floors, phones should be put away. If pupils in Sixth Form are on their phones outside of their designated areas, their phone will be confiscated. The pupil will receive 1 misdemeanour and the phone must be handed into the Head of Year for the following 2 weeks.
- Parents wishing to contact their children in an emergency should always telephone the School Office and a message will be relayed promptly.
- Pupils may not bring mobile phones, Smart Watches or any other wearables into examination rooms under any circumstances. If brought into the exam room by the pupil, they must be handed in before the exam starts, and then collected after the examination.
- Pupils permitted to bring mobile phones onto School premises may only use it during School hours with the express permission from their subject teacher, Head of School or Housemistress and they may be supervised. In emergencies, pupils may request to use the school telephone.
- Pupils must not use mobile phones in any manner which in the reasonable opinion of the Principal is inappropriate. The taking and storing of indecent images and sexting are serious breaches of discipline and safeguarding issues. Any incident of this nature will not be tolerated and will constitute a serious breach of discipline.
- The School reserves the right to confiscate a pupil's mobile phone for a specified period of time if the pupil is found to be in breach of this policy. The mobile may be searched in appropriate circumstances (see the School's *Behaviour Policy).* The pupil may also be prevented from

bringing a mobile phone into the School temporarily or permanently and at the sole discretion of the Principal.

- Pupils should not use mobile phones to communicate with staff via staff's personal electronic devices. If there are reasonable grounds to believe that inappropriate communications have taken place, the Principal will require the relevant devices to be produced for examination and the usual disciplinary procedures will apply. Staff on school trips and House staff are provided with School phones in order to communicate with pupils.

Appendix 4 Camera, photograph and video protocol

- Lower School and Lower 5 Pupils are not allowed to operate mobile phones (including cameras on their phones), or have them on their person during school hours. If a pupil in Lower School or Lower 5 is found in possession of a phone during the School day, they will receive an instant detention, on Friday after school, 4.45 to 5.45.
- All pupils must not use cameras or other devices with the capability for recording and/or storing still or moving images without the express permission of the member of staff in charge and of those appearing in the image.
- Using photographic material of any kind to bully, harass, undermine or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- All pupils must allow members of the School's Senior Leadership Team to access images stored on mobile phones and/or cameras and must delete images if requested to do so. This would only be done if the School had reason to believe that the image constitutes a breach of the School's online safety or behaviour policies.
- Posting of photographic material which in the reasonable opinion of the Principal is considered to be offensive on websites such as YouTube, Instagram, Tik Tok, Facebook, Twitter etc. is a serious breach of the online safety policy and will be subject to disciplinary procedures whatever the source of the material. This is the position whether the device used is a School computer, or a device operated elsewhere including the pupil's home.
- Cameras and mobile electronic devices with a camera facility may be confiscated and searched in appropriate circumstances (see the School's *Behaviour Policy*). If the Principal has reasonable grounds to believe that a pupil's camera or mobile electronic device contains images, text messages or other material that may constitute evidence of criminal activity, she may hand the device to the Police for examination.
- Use of cameras, mobile electronic devices with camera facilities or laptop computers in breach of this policy may result in the immediate confiscation of the device and further disciplinary action being taken. Depending on the breach, disciplinary action could include: misdemeanours (-5), long term removal of device privileges, detention or suspension from school, (internal or external).

Earphones/AirPods Protocol

If a pupil wears earphones/AirPods, during the school day, the pupil will receive 1 misdemeanour.

If a pupil wears earphones/AirPods, during Chapels, Assemblies, lessons, or in the dining room the pupil will receive an instant detention, on Friday after school, 4.45 to 5.45.

Appendix 5 Personal Safety

Pupils must not:

- Pupils must not use any type of social media to interact with people that they do not know in person;
- Reveal their home address, image, or phone numbers, or those of other pupils or of staff when on-line. They must use school addresses and phone numbers only;
- Arrange to meet someone that they have only met on the Internet or by email or in a chat room.
- Share their network password or allow others to use it;

Pupils must:

- Use only their account and keep their password private;Create a strong password, with at least 8 characters and at least one number with either a capital or a symbol. Pupils must never share their passwords with others and must ensure that they log off when leaving their PC;
- Report to a system administrator, teacher or administrator any unsolicited email, security problems, any unpleasant or inappropriate material, messages, or anything that makes them feel uncomfortable when on-line;
- Use social and blogging websites with great care being aware of the dangers that can be associated with posting pictures, text, opinions, videos and communications on-line. All social networking sites such as Facebook, Twitter and qq.com are restricted as explained in section 11 'Use of Social Networks';
- Make themselves aware of the security settings available when using social and blogging websites to protect personal information which is published on-line.

Cyber-bullying

Cyberbullying is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Any behaviour which seeks to intimidate or humiliate and which is repeated, intentional, malicious, such as to cause distress, unhappiness or insecurity, is strictly forbidden, and is considered to be a serious breach of discipline.

Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

On the School's SharePoint homepage there is a link to https://www.thinkuknow.co.uk/ the education programme from NCA-CEOP, a UK organisation which protects children both online and offline.

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.

- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Do not retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to evidence what is happening and can be used by the School to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving inappropriately.
- It is important to act. In the event that a pupil witnesses cyberbullying, it is important to support the victim and report the bully.

Guidance for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The procedures below should be followed:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police (Please refer to the School's *Safeguarding and Child Protection Policy* for further information). Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

If any pupil thinks that they, or another person, is being bullied, they should talk to a teacher or any trusted adult about the incident as soon as possible. For further guidance, see the School's Anti-bullying Policy.

The website http://www.digizen.org/kids/ also provides useful support and resources to pupils who may feel uncomfortable with their use of the Internet. Other useful resources include:

- https://www.internetmatters.org/
- https://www.ceop.police.uk/safety-centre/
- https://www.issuesonline.co.uk/subscription/login
- http://www.saferinternet.org.uk/
- http://www.kidsmart.org.uk
- http://www.safetynetkids.org.uk/
- http://www.safekids.com/
- http://www.thinkuknow.co.uk

Safeguarding and Prevent

The school recognises that it has a duty under Section 26 of the Counter-Terrorism and Security Act (2015) to have due regard to the need to prevent people from being drawn into terrorism and to promote and safeguard the welfare of children and vulnerable adults (Education Act 2002, KCSIE 2024).

Staff are responsible for the well-being of the pupils and must ensure age-appropriate material only is accessible via the school network by the use of filters. Any member of staff who feels someone is showing an interest in extremist, abusive or inappropriate material should report this to the DSL in the first instance.

Any member of staff who believes pupils have access to inappropriate material should report this to the IT manager.

Guidelines for boarders

Boarding pupils are subject to all of the provisions in this policy at all times. Pupils may use the sockets or wireless network available in each of the boarding houses to remotely log on to the School system and use the Internet. This access is monitored by the Housemistress or Assistant Housemistress and may be suspended, at their discretion, if it is believed that a girl is spending too much time on the Internet.

Lower School Devices

Lower School are expected to hand in all electronic devices to the staff member on duty, each evening, from Sunday to Thursday. These times are outlined below:

Year Group	Device hand in time
• Upper 3	8.30PM
• Lower 4	8.45PM
• Upper 4	9.00PM
• Lower 5	9.15PM
• Upper 5	9.30PM

Devices can be collected from the Housemistresses Office each morning.

Internet access is available as follows:

Year Group	Internet Access Times
• Upper 3	• 6.00am – 8.30pm each weekday (Sunday to Thursday) • 6.00am – 10.00pm on weekends (Friday and Saturday)
• Lower 4	• 6.00am – 9.00pm each weekday (Sunday to Thursday) • 6.00am – 10.00pm on weekends (Friday and Saturday)
• Upper 4	• 6.00am – 9.30pm each weekday (Sunday to Thursday) • 6.00am – 10.00pm on weekends (Friday and Saturday)
• Lower 5	• 6.00am – 10.00pm every day
• Upper 5	• 6.00am – 10.30pm every day
• Sixth Form	• 6.00am – 11.00pm every day

- After 7.00pm, access to approved recreational sites is permitted on the boarding computing facilities. Requests for particular sites to be made available should be directed to the Housemistress or Assistant Housemistress in the first instance;
- Connection to the Internet will be disabled every night in accordance with the timetable above;
- All activity on the School's computing facilities is monitored, which will alert the ICT department to any breaches of this policy;
- Pupils are welcome to use their own electronic devices capable of connecting to a wireless network, including laptops, tablet computers, iPods and mobile phones but these should only be connected to the School's network. Connection to the internet via a mobile service is not permitted. Please contact the Network Services Department by telephone for further information.

- Middle School and Sixth Form pupils should ensure all mobile phones (6th Form) and tablets are turned off at the end of the day. These times are in line with the Internet access times for their year group and are shown in the table above;
- Please refer to the Boarders' Handbook for further information about communication in the boarding houses.

Appendix 6 Online Learning

If a pupil cannot attend School, but is well enough to engage in learning, the pupil should engage with HLC's remote learning provision, and complete the work set.

If a pupil is remote learning, they are expected to contact their teachers and check for work, and prep on the School's VLE.

In the event of a full, or partial, School closure, pupils will have access to remote lessons and are expected to follow the expectations outlined in the Remote Education Policy.

1. **Printing**
2. All pupils are allowed a set number of printer credits for the year, these are allocated on a monthly basis. Pupils who use more than their monthly allocation may request more credits by contacting 'support@hlc.org.uk'. Any additional credits will be taken from the following months' allocation. Credits are shown as a cost in pounds and pence with a black and white print costing approximately 1p and a colour print costing approximately 8p per page of A4.**Procedures**

Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. Violations of the rules in this policy will be dealt with in accordance with the School's Behaviour Policy.

Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Policy.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures outlined in the School's Safeguarding and Child Protection Policy. If a pupil is worried about something that he/she has seen on the internet, he/ she should talk to a teacher about it as soon as possible.

3. Sanctions

Pupils are expected to adhere to this policy at all times. Violations of the rules in this policy will result in a temporary or permanent ban from the School network. Additional disciplinary action may be taken, in accordance with the School's Behaviour Policy and will depend upon the seriousness of the offence. Teachers are not expected to give verbal warnings prior to implementing a sanction. Depending on the breach, disciplinary action could include, but is not limited to: misdemeanours (-5), long term removal of device privileges, detention or suspension from school, (internal or external). When applicable, the Police or local authorities may be involved.

The School reserves the right to charge a pupil or his / her parents for any costs incurred to the School, or to indemnify any significant liability incurred by the School, as a result of a breach of this policy.

Appendix 7 Online Safety Incident Reporting Form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the DSL.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age-inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	

Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix 8 Rationale for Acceptable Use Agreement (AUA) for all College Pupils

The internet, email, mobile technologies and online resources are an important part of learning and life. We aim to ensure that all pupils at HLC are safe and responsible users of IT. It is essential that pupils are aware of online risk, know how to stay safe and know where to go to report problems and access support.

Harrogate Ladies' College is fully committed to enabling all pupils to access technology to enhance teaching and learning within a safe and secure environment. Technology is an important element of HLC's teaching and forms an integral part of a modern curriculum. The School seeks to raise the standard of each pupil's digital competence through regular opportunities to use technology within their studies.

HLC provides computer facilities and other technology for use by pupils. The computers are provided and maintained for the benefit of everyone. All pupils are encouraged to use and enjoy these resources and help to ensure they remain available to all. Similarly, pupils who use their own devices in College are expected to use their devices responsibly and adhere to the expectations outlined in this AUA.

Pupils are responsible for good behaviour with the resources provided. Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

This AUA outlines the rules designed to keep all pupils safe now and in the future. All pupils in College electronically sign this AUA when they log onto the HLC Internet. This Agreement applies to pupil's use of all ICT systems.

If a pupil breaks the rules outlined, relevant staff will investigate. Pupils may be disciplined, and parents/carers may be contacted. If pupils break the law the police will be informed.

Acceptable Use Agreement (AUA)

To access the School's IT systems, it is important that you adhere to the expectations in this AUA. These are outlined below and categorized into 6 key areas:

- Use of school equipment
- Use of your own equipment
- Passwords and security
- Internet searches, filtering and monitoring
- Communications and sharing, including social media use
- Plagiarism and use of AI

If you break any of the rules and expectations outlined in this AUA, relevant staff will investigate. You may be disciplined in accordance with this AUA, the Online Safety Policy, the Artificial Intelligence (AI) Policy and the School's Behaviour Policy. Parents, guardians and/or carers may be contacted. In the event that a pupil breaks the law, the police will be informed.

Use of school equipment

1. I will not behave in a way that can cause damage to school ICT equipment or to IT installations. I will not change any of the computers' default settings, such as: screensavers, backgrounds, folders and/or icons.

2. I will only use the school computers for educational purposes and will not download or install software onto school devices.

3. I will not intentionally waste resources, for example with regards to printing.

4. I will only use school IT equipment for school purposes.

5. I will not use my personal email address or other personal accounts to sign into any school resources

Use of own equipment

1. I take full responsibility for keeping my device secure whilst at School. When it is not on my person, I will ensure that it is kept in a lockable space.

2. Whilst on the School premises, I will only connect my device to the school's guest network. I understand that no VPNs, dongles or mobile networks are acceptable for use in school.

3. External media types such as memory sticks or CD's are prohibited unless approved by ICT Support

4. I will not assume that new technologies can be brought into school and will check with ICT Support before bringing in any device.

5. I will only use mobile devices in class with my teacher's permission, and only then for school-related work.

6. Under no circumstances should School computers, printers or other devices be detached from the network to make way for my own device.

Passwords and security

1. I will create a strong password, with at least 8 characters and at least one number with either a capital or a symbol.

2. I will not share my passwords with others and will always ensure that I log off when leaving a PC.

3. I will only log on to the school network/office 365/SharePoint with my own username and password. I will keep my password secret, and ensure it is secure and updated regularly.

4. I will not attempt to log on using another person's username and password with or without their permission. I will not use another person's account. I will not access another person's device or storage area, or interfere with other people's work or files

5. I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will report immediately any request for personal information to a member of staff if I am in school, or parent/carer if I am not in school.

6. I will not lie about my age in order to sign up for age inappropriate games, apps or social networks.

7. I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk.

Internet searches, filtering and monitoring

1. I will be responsible for my behaviour when using the Internet and other school resources.

2. I will not attempt to bypass the Internet filtering system or circumvent any security features of the school network. The use of routers, dongles and VPNs are banned in School.

3. I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.

4. I will ensure that my online activity, both in school and outside school will not cause the school, staff or other pupils' distress and it will not defame, undermine, misrepresent or tarnish the reputation of the school and its users.

5. I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it to a member of staff immediately, or parent/carer if I am not in school.

Communications and sharing, including social media use

1. I will always use my school email address for school communications including contact with other students, teachers and staff.

2. I will make sure that all my electronic communications are responsible and sensible. The messages I send will be polite, respectful and responsible.

3. I will only contact my teachers, and the staff at HLC, using school email. All emails will be written in a professional and courteous manner. I will not use **any** social media platform to contact staff at HLC.

4. I understand that the use of social networking sites such as Instagram, TikTok Facebook, Twitter, qq.com or similar sites is prohibited during the school day. Access is only available between 7.00am and 7.30am and after 7.00pm and is restricted to pupils in Upper 5 or older.

5. I will never post photographs, videos or livestream without the permission of all parties involved.

6. I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.

7. I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying.

8. I will not respond to hurtful behaviour online but will report it. I have the right to block any inappropriate or upsetting request.

Plagiarism and use of AI

1. I will respect the privacy and ownership of others' work on-line at all times and will not take information from the Internet and pass it off as my own work. I will adhere to copyright at all times.

2. I will not use AI to produce work and pass off ideas, text, images or other outputs produced by AI as my own.

3. Whenever AI, Internet or other sources have been used to produce my work, I must include a clear acknowledgement of how these sources have been used.